# Indefinite Integration – an Arithmetic Approach

An Effective Version of the Grothendieck $p$-curvature Conjecture for Order One Differential Equations

joint work with L. Pannier, arXiv:2510.00892

Florian Fürnsinn

University of Vienna

Pascaline Seminar, LIP, ENS de Lyon

October 16, 2025

# Overview

1. Power Series, Algebraicity and Differential Equations
2. Order One Equations and a Theorem of Kronecker
3. An Effective Version of Kronecker's Theorem
4. Effective Version of the $p$-Curvature Conjecture for Order 1 Equations
5. Different Approaches to the Problem

# A Hierarchy of Power Series

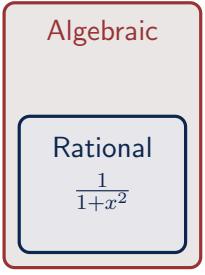
# A Hierarchy of Power Series

Rational

$\frac{1}{1+x^2}$

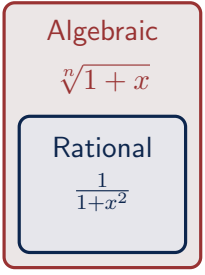
# A Hierarchy of Power Series

A power series $f(x) \in \mathbb{Q}[\![x]\!]$ is called **algebraic**, if it is annihilated by a non-zero polynomial $P(x, y) \in \mathbb{Q}[x, y]$, i.e., $P(x, f(x)) = 0$.



# A Hierarchy of Power Series

A power series $f(x) \in \mathbb{Q}[\![x]\!]$ is called **algebraic**, if it is annihilated by a non-zero polynomial $P(x, y) \in \mathbb{Q}[x, y]$, i.e., $P(x, f(x)) = 0$.

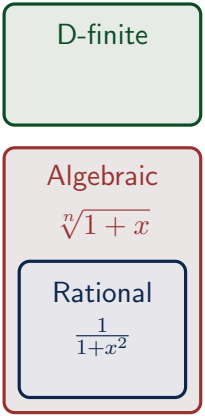


# A Hierarchy of Power Series

A power series $f(x) \in \mathbb{Q}[\![x]\!]$ is called **algebraic**, if it is annihilated by a non-zero polynomial $P(x, y) \in \mathbb{Q}[x, y]$, i.e., $P(x, f(x)) = 0$.

A power series $f(x) \in \mathbb{Q}[\![x]\!]$ is called **D-finite**, if it satisfies a non-zero linear differential equation with polynomial coefficients $a_i(x) \in \mathbb{Q}[x]$:

$$a_n(x)f^{(n)}(x) + a_{n-1}(x)f^{(n-1)}(x) + \cdots + a_0(x)f(x) = 0.$$

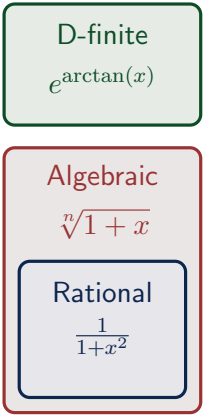


# A Hierarchy of Power Series

A power series $f(x) \in \mathbb{Q}[\![x]\!]$ is called **algebraic**, if it is annihilated by a non-zero polynomial $P(x, y) \in \mathbb{Q}[x, y]$, i.e., $P(x, f(x)) = 0$.

A power series $f(x) \in \mathbb{Q}[\![x]\!]$ is called **D-finite**, if it satisfies a non-zero linear differential equation with polynomial coefficients $a_i(x) \in \mathbb{Q}[x]$:

$$a_n(x)f^{(n)}(x) + a_{n-1}(x)f^{(n-1)}(x) + \cdots + a_0(x)f(x) = 0.$$



# A Hierarchy of Power Series

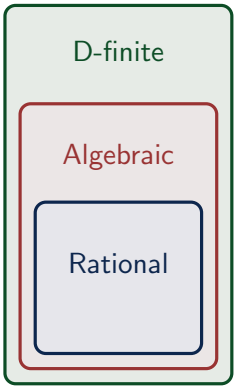
A power series $f(x) \in \mathbb{Q}[\![x]\!]$ is called **algebraic**, if it is annihilated by a non-zero polynomial $P(x, y) \in \mathbb{Q}[x, y]$, i.e., $P(x, f(x)) = 0$.

A power series $f(x) \in \mathbb{Q}[\![x]\!]$ is called **D-finite**, if it satisfies a non-zero linear differential equation with polynomial coefficients $a_i(x) \in \mathbb{Q}[x]$:

$$a_n(x)f^{(n)}(x) + a_{n-1}(x)f^{(n-1)}(x) + \cdots + a_0(x)f(x) = 0.$$

**Theorem (Folklore; Abel 1829)**

*Every algebraic power series is D-finite.*



# A Hierarchy of Power Series

A power series $f(x) \in \mathbb{Q}[\![x]\!]$ is called **algebraic**, if it is annihilated by a non-zero polynomial $P(x, y) \in \mathbb{Q}[x, y]$, i.e., $P(x, f(x)) = 0$.

A power series $f(x) \in \mathbb{Q}[\![x]\!]$ is called **D-finite**, if it satisfies a non-zero linear differential equation with polynomial coefficients $a_i(x) \in \mathbb{Q}[x]$:

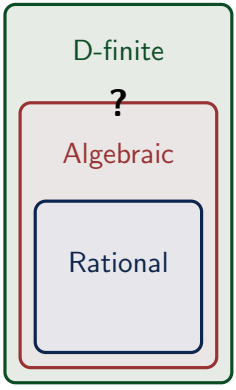
$$a_n(x)f^{(n)}(x) + a_{n-1}(x)f^{(n-1)}(x) + \cdots + a_0(x)f(x) = 0.$$

**Theorem (Folklore; Abel 1829)**

*Every algebraic power series is D-finite.*

**Question (Fuchs, Liouville, Stanley)**

Which D-finite series are algebraic?



# Algebraicity of Integrals

## Special Case

When is the solution of $y'(x) = u(x)$ for a rational function $u(x) \in \mathbb{Q}(x)$ algebraic?

# Algebraicity of Integrals

## Special Case

When is the solution of $y'(x) = u(x)$ for a rational function $u(x) \in \mathbb{Q}(x)$ algebraic?

Note: $y(x)$ is D-finite, although we are only given an **inhomogeneous** differential equation.

# Algebraicity of Integrals

## Special Case

When is the solution of $y'(x) = u(x)$ for a rational function $u(x) \in \mathbb{Q}(x)$ algebraic?

Note: $y(x)$ is D-finite, although we are only given an **inhomogeneous** differential equation.

Partial fraction decomposition of $u(x)$:

$$u(x) = \sum_{i,j} \frac{\beta_{i,j}}{(x - \alpha_i)^j} + P(x).$$

Then $y(x)$ is **rational** (and thus **algebraic**) if and only if $\beta_{i,1} = 0$ for all $i$. Otherwise: summands of the form $\beta_{i,j} \cdot \log(x - \alpha_i)$ appear, and $y(x)$ is **transcendental**.

# Algebraicity of Integrals

## Special Case

When is the solution of $y'(x) = u(x)$ for an **algebraic** function $u(x) \in \mathbb{Q}[\![x]\!]$ algebraic?

A power series $f(x) \in \mathbb{Q}[\![x]\!]$ is called **globally bounded** (g.b.) if there exist $\alpha, \beta \in \mathbb{Z} \setminus \{0\}$, such that $\alpha f(\beta x) \in \mathbb{Z}[\![x]\!]$.

# Algebraicity of Integrals

## Special Case

When is the solution of $y'(x) = u(x)$ for an **algebraic** function $u(x) \in \mathbb{Q}[\![x]\!]$ algebraic?

A power series $f(x) \in \mathbb{Q}[\![x]\!]$ is called **globally bounded** (g.b.) if there exist $\alpha, \beta \in \mathbb{Z} \setminus \{0\}$, such that $\alpha f(\beta x) \in \mathbb{Z}[\![x]\!]$.

## Theorem (André, 1989)

*The primitive $y(x)$ of an algebraic function $u(x)$ is algebraic if and only if it is g.b.*

# Algebraicity of Integrals

## Special Case

When is the solution of $y'(x) = u(x)$ for an **algebraic** function $u(x) \in \mathbb{Q}[\![x]\!]$ algebraic?

A power series $f(x) \in \mathbb{Q}[\![x]\!]$ is called **globally bounded** (g.b.) if there exist $\alpha, \beta \in \mathbb{Z} \setminus \{0\}$, such that $\alpha f(\beta x) \in \mathbb{Z}[\![x]\!]$.

## Theorem (André, 1989)

*The primitive $y(x)$ of an algebraic function $u(x)$ is algebraic if and only if it is g.b.*

André's Theorem provides an **arithmetic** characterization of algebraicity of primitives.

# Algebraicity of Integrals

## Special Case

When is the solution of $y'(x) = u(x)$ for an **algebraic** function $u(x) \in \mathbb{Q}[\![x]\!]$ algebraic?

A power series $f(x) \in \mathbb{Q}[\![x]\!]$ is called **globally bounded** (g.b.) if there exist $\alpha, \beta \in \mathbb{Z} \setminus \{0\}$, such that $\alpha f(\beta x) \in \mathbb{Z}[\![x]\!]$.

## Theorem (André, 1989)

*The primitive $y(x)$ of an algebraic function $u(x)$ is algebraic if and only if it is g.b.*

André's Theorem provides an **arithmetic** characterization of algebraicity of primitives.

## Example

The series $\int \frac{1}{1-x} = \int 1 + x + x^2 + \ldots = x + \frac{x^2}{2} + \frac{x^3}{3} + \ldots = -\log(1-x)$ is not g.b.

# Algebraicity of Logarithmic Integrals

## Homogeneous Equations of Order One

When is the solution of $y'(x) = u(x)y(x)$ for a rational function $u(x) \in \mathbb{Q}(x)$ algebraic?

# Algebraicity of Logarithmic Integrals

## Homogeneous Equations of Order One

When is the solution of $y'(x) = u(x)y(x)$ for a rational function $u(x) \in \mathbb{Q}(x)$ algebraic?

Solution $y(x) = \exp\left(\int u(x)\mathrm{d}x\right)$. Partial fraction decomposition of $u(x)$:

$$u(x) = \sum_{i,j} \frac{\beta_{i,j}}{(x-\alpha_i)^j} + P(x).$$

Write

$$R(x) = \int \sum_{j>1,i} \frac{\beta_{i,j}}{(x-\alpha_i)^j} + P(x)\ \mathrm{d}x \in \mathbb{Q}(x).$$

Then

$$y(x) = \prod (x-\alpha_i)^{\beta_{i,1}} \cdot \exp(R(x))$$

is algebraic if and only if $\beta_{i,1} \in \mathbb{Q}$ and $R(x) = 0$.

# Algebraicity of Logarithmic Integrals

## Homogeneous Equations of Order One

When is the solution of $y'(x) = u(x)y(x)$ for an **algebraic** function $u(x) \in \mathbb{Q}[\![x]\!]$ algebraic?

This is known as **Abel's Problem**.

# Algebraicity of Logarithmic Integrals

## Homogeneous Equations of Order One

When is the solution of $y'(x) = u(x)y(x)$ for an **algebraic** function $u(x) \in \mathbb{Q}[\![x]\!]$ algebraic?

This is known as **Abel's Problem**.

It is more involved, as there is no easy analogue of the partial fraction decomposition for algebraic power series.

# Algebraicity of Logarithmic Integrals

## Homogeneous Equations of Order One

When is the solution of $y'(x) = u(x)y(x)$ for an **algebraic** function $u(x) \in \mathbb{Q}[\![x]\!]$ algebraic?

This is known as **Abel's Problem**.

It is more involved, as there is no easy analogue of the partial fraction decomposition for algebraic power series.

It was solved by Risch in 1970, and by Baldassari and Dwork in 1979.

# Deciding Algebraicity of D-Finite Series

## Deciding Algebraicity

Given a linear differential equation with polynomial coefficients, decide if (A) all solutions are algebraic, (E) there is a non-zero algebraic solution, or (P) a particular solution is algebraic.

# Deciding Algebraicity of D-Finite Series

## Deciding Algebraicity

Given a linear differential equation with polynomial coefficients, decide if (A) all solutions are algebraic, (E) there is a non-zero algebraic solution, or (P) a particular solution is algebraic.

Question (A) solved by Singer 1979, relying on Risch's algorithm for Abel's Problem, and earlier work by Painlevé (1887) and Boulanger (1898). It involves exponential bounds, and is not suitable for implementation.

# Deciding Algebraicity of D-Finite Series

## Deciding Algebraicity

Given a linear differential equation with polynomial coefficients, decide if (A) all solutions are algebraic, (E) there is a non-zero algebraic solution, or (P) a particular solution is algebraic.

Question (A) solved by Singer 1979, relying on Risch's algorithm for Abel's Problem, and earlier work by Painlevé (1887) and Boulanger (1898). It involves exponential bounds, and is not suitable for implementation.

Recent (semi-)algorithms for question (P) [Bostan, Salvy, Singer, 2025+].

# Deciding Algebraicity of D-Finite Series

## Deciding Algebraicity

Given a linear differential equation with polynomial coefficients, decide if (A) all solutions are algebraic, (E) there is a non-zero algebraic solution, or (P) a particular solution is algebraic.

Question (A) solved by Singer 1979, relying on Risch's algorithm for Abel's Problem, and earlier work by Painlevé (1887) and Boulanger (1898). It involves exponential bounds, and is not suitable for implementation.

Recent (semi-)algorithms for question (P) [Bostan, Salvy, Singer, 2025+].

Special cases are easier: e.g. order one (as discussed before), or hypergeometric functions [Christol, 1986; Beukers-Heckman 1989; F.-Yurkevich 2024]

# An Arithmetic Approach – A Local-Global Principle

$$a_n(x)f^{(n)}(x) + a_{n-1}(x)f^{(n-1)}(x) + \cdots + a_0(x)f(x) = 0 \quad \text{with } a_i \in \mathbb{Q}[x] \qquad (*)$$

To a differential equation $(*)$ one can associate for each prime $p$ a matrix, the **$p$-curvature**.

# An Arithmetic Approach – A Local-Global Principle

$$a_n(x)f^{(n)}(x) + a_{n-1}(x)f^{(n-1)}(x) + \cdots + a_0(x)f(x) = 0 \quad \text{with } a_i \in \mathbb{Q}[x] \qquad (*)$$

To a differential equation $(*)$ one can associate for each prime $p$ a matrix, the **$p$-curvature**.

**Theorem (Cartier's Lemma, [Katz 1972])**

*The $p$-curvature of $(*)$ vanishes if and only if it has a basis of $n$ solutions in $\mathbb{F}_p[\![x]\!]$.*

# An Arithmetic Approach – A Local-Global Principle

$$a_n(x)f^{(n)}(x) + a_{n-1}(x)f^{(n-1)}(x) + \cdots + a_0(x)f(x) = 0 \quad \text{with } a_i \in \mathbb{Q}[x] \qquad (*)$$

To a differential equation $(*)$ one can associate for each prime $p$ a matrix, the **$p$-curvature**.

**Theorem (Cartier's Lemma, [Katz 1972])**

*The $p$-curvature of $(*)$ vanishes if and only if it has a basis of $n$ solutions in $\mathbb{F}_p[\![x]\!]$.*

**Grothendieck $p$-Curvature Conjecture, 1969**

All solutions of $(*)$ are algebraic if and only if for almost all prime numbers $p$ the $p$-curvature of $(*)$ vanishes.

# An Arithmetic Approach – A Local-Global Principle

$$a_n(x)f^{(n)}(x) + a_{n-1}(x)f^{(n-1)}(x) + \cdots + a_0(x)f(x) = 0 \quad \text{with } a_i \in \mathbb{Q}[x] \qquad (*)$$

To a differential equation $(*)$ one can associate for each prime $p$ a matrix, the **$p$-curvature**.

**Theorem (Cartier's Lemma, [Katz 1972])**

*The $p$-curvature of $(*)$ vanishes if and only if it has a basis of $n$ solutions in $\mathbb{F}_p[\![x]\!]$.*

**Grothendieck $p$-Curvature Conjecture, 1969**

All solutions of $(*)$ are algebraic if and only if for almost all prime numbers $p$ the $p$-curvature of $(*)$ vanishes.

Proven: Picard-Fuchs equations [Katz 1972], **Order one** [Honda, 1981; Chudnovsky$^2$, 1985].

# An Arithmetic Approach – A Local-Global Principle

$$a_n(x)f^{(n)}(x) + a\ldots(x)f^{(n-1)}(x) + \ldots + a_0(x)f(x) = 0 \quad \text{with } a_i \in \mathbb{Q}[x] \qquad (*)$$

To a differential equation (∗) … matrix, the **$p$-curvature**.

**Theorem (Cartier's Lemm…**

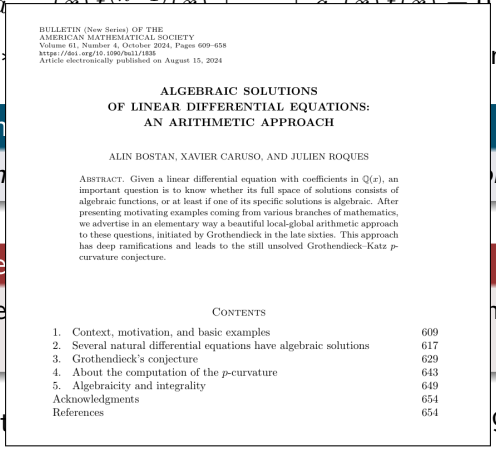
*The $p$-curvature of (∗) van… …lutions in $\mathbb{F}_p[\![x]\!]$.*

**Grothendieck $p$-Curvature…**

All solutions of (∗) are alge… …numbers $p$ the $p$-curvature of (∗) vanishes.

Proven: Picard-Fuchs equat… …981; Chudnovsky[2], 1985].

Recent expository paper [Bostan, Caruso, Roques, 2024].



BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 61, Number 4, October 2024, Pages 609–658
https://doi.org/10.1090/bull/1838
Article electronically published on August 15, 2024

**ALGEBRAIC SOLUTIONS OF LINEAR DIFFERENTIAL EQUATIONS: AN ARITHMETIC APPROACH**

ALIN BOSTAN, XAVIER CARUSO, AND JULIEN ROQUES

ABSTRACT. Given a linear differential equation with coefficients in $\mathbb{Q}(x)$, an important question is to know whether its full space of solutions consists of algebraic functions, or at least if one of its specific solutions is algebraic. After presenting motivating examples coming from various branches of mathematics, we advertise in an elementary way a beautiful local-global arithmetic approach to these questions, initiated by Grothendieck in the late sixties. This approach has deep ramifications and leads to the still unsolved Grothendieck–Katz $p$-curvature conjecture.

CONTENTS

# Back to Order One Equations

**Theorem (Jacobson, 1937)**

*The $p$-curvature of the equation $y'(x) = u(x) \cdot y(x)$ is given by $u(x)^p + u^{(p-1)}(x) \in \mathbb{F}_p(x)$.*

# Back to Order One Equations

**Theorem (Jacobson, 1937)**

*The $p$-curvature of the equation $y'(x) = u(x) \cdot y(x)$ is given by $u(x)^p + u^{(p-1)}(x) \in \mathbb{F}_p(x)$.*

**Recall**

*A solution of an order one differential equation $y'(x) = u(x)y(x)$ is given by*

$$y(x) = \exp\left(\int u(x)\mathrm{d}x\right).$$

# Examples

## Example

The equation $y'(x) = y(x)$ has no solution in $\mathbb{F}_p[\![x]\!]$, and $\exp(x)$ is transcendental. Moreover, $1^p + 1^{(p-1)} = 1 \neq 0$ for all primes $p$.

# Examples

## Example

The equation $y'(x) = y(x)$ has no solution in $\mathbb{F}_p[\![x]\!]$, and $\exp(x)$ is transcendental. Moreover, $1^p + 1^{(p-1)} = 1 \neq 0$ for all primes $p$.

## Example

The function $y(x) = \exp(\arctan(x))$ satisfies $y'(x) = \frac{1}{1+x^2} \cdot y(x)$. We have

$$u(x)^p + u^{(p-1)}(x) = \begin{cases} 0 & \text{if } p \equiv 1 \bmod 4 \\ \frac{2}{(x+1)^p} & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

So $y(x)$ is not algebraic.

# Kronecker's Theorem

**Theorem (Kronecker, 1880)**

*Let $R(w) \in \mathbb{Q}[w]$. Assume that the reduction of $R(w)$ modulo $p$ splits into linear factors in $\mathbb{F}_p[w]$ for almost all prime numbers $p$. Then $R(w)$ splits into linear factors in $\mathbb{Q}[w]$.*

**Example**

The polynomial $x^2 + 1 \in \mathbb{F}_p[x]$ factors as $(x + i)(x - i) \in \mathbb{F}_p[x]$ for $p \equiv 1 \bmod 4$ and is irreducible if $p \equiv 3 \bmod 4$, as $-1 \in \mathbb{F}_p$ is a square precisely in the first case.

# Kronecker's Theorem

**Theorem (Kronecker, 1880)**

*Let $R(w) \in \mathbb{Q}[w]$. Assume that the reduction of $R(w)$ modulo $p$ splits into linear factors in $\mathbb{F}_p[w]$ for almost all prime numbers $p$. Then $R(w)$ splits into linear factors in $\mathbb{Q}[w]$.*

**Example**

The polynomial $x^2 + 1 \in \mathbb{F}_p[x]$ factors as $(x + i)(x - i) \in \mathbb{F}_p[x]$ for $p \equiv 1 \bmod 4$ and is irreducible if $p \equiv 3 \bmod 4$, as $-1 \in \mathbb{F}_p$ is a square precisely in the first case.

Nowadays, this theorem is seen as a consequence of Chebotarev's Density Theorem.

# Kronecker's Theorem

**Theorem (Kronecker, 1880)**

*Let $R(w) \in \mathbb{Q}[w]$. Assume that the reduction of $R(w)$ modulo $p$ splits into linear factors in $\mathbb{F}_p[w]$ for almost all prime numbers $p$. Then $R(w)$ splits into linear factors in $\mathbb{Q}[w]$.*

**Example**

The polynomial $x^2 + 1 \in \mathbb{F}_p[x]$ factors as $(x + i)(x - i) \in \mathbb{F}_p[x]$ for $p \equiv 1 \bmod 4$ and is irreducible if $p \equiv 3 \bmod 4$, as $-1 \in \mathbb{F}_p$ is a square precisely in the first case.

Nowadays, this theorem is seen as a consequence of Chebotarev's Density Theorem.

A different proof was given by Chudnovsky[2] in 1985 using Hermite-Padé approximation.

# Rothstein-Trager Resultants

**Theorem (Rothstein, 1976; Trager, 1976)**

*Let $u(x) \in \mathbb{Q}(x)$ be a rational function of the form*

$$u(x) = \frac{a(x)}{b(x)} = \sum_{i=1}^{r} \frac{\alpha_i}{x - \beta_i},$$

*with $a(x), b(x) \in \mathbb{Z}[x]$. Then the residues $\alpha_i$ are precisely the roots of*

$$R(w) \coloneqq \mathrm{Res}_x(b(x), a(x) - w \cdot b'(x)) \in \mathbb{Z}[w].$$

# Proof of Honda's Theorem

$$y'(x) = u(x)y(x) \quad \text{(Eq)} \quad \text{with } u(x) = \frac{a(x)}{b(x)}, \text{ and } R(w) \coloneqq \operatorname{Res}(b(x), a(x) - w \cdot b'(x)).$$

**Proposition (Folklore; Honda, 1981)**

*The following are equivalent:*

(1) (Eq) *has an algebraic solution.*

(2) *We have* $\deg a(x) < \deg b(x)$*, all poles of* $u(x)$ *are simple, and* $R(w)$ *splits completely in* $\mathbb{Q}[w]$.

# Proof of Honda's Theorem

$$y'(x) = u(x)y(x) \quad \text{(Eq)} \quad \text{with } u(x) = \frac{a(x)}{b(x)}, \text{ and } R(w) \coloneqq \operatorname{Res}(b(x), a(x) - w \cdot b'(x)).$$

**Proposition (Folklore; Honda, 1981)**

*The following are equivalent:*

(1) (Eq) *has an algebraic solution.*
(2) *We have* $\deg a(x) < \deg b(x)$*, all poles of* $u(x)$ *are simple, and* $R(w)$ *splits completely in* $\mathbb{Q}[w]$.

**Proposition (Honda, 1981)**

*Let* $p$ *be a prime number. TFAE:*

($1_p$) $(\text{Eq})_p$ *has an algebraic solution in* $\mathbb{F}_p[\![x]\!]$.
($2_p$) *We have* $\deg a(x) < \deg b(x)$*, all poles of* $u(x)$ *are simple, and* $R(w)$ *splits completely in* $\mathbb{F}_p[w]$.
($3_p$) *We have* $u(x)^p + u^{(p-1)}(x) = 0$.

# Proof of Honda's Theorem

$$y'(x) = u(x)y(x) \quad \text{(Eq)} \quad \text{with } u(x) = \frac{a(x)}{b(x)}, \text{ and } R(w) \coloneqq \operatorname{Res}(b(x), a(x) - w \cdot b'(x)).$$

**Proposition (Folklore; Honda, 1981)**

*The following are equivalent:*

(1) (Eq) *has an algebraic solution.*

(2) *We have* $\deg a(x) < \deg b(x)$*, all poles of* $u(x)$ *are simple, and* $R(w)$ *splits completely in* $\mathbb{Q}[w]$.

**Proposition (Honda, 1981)**

*Let* $p$ *be a prime number. TFAE:*

($1_p$) $(\text{Eq})_p$ *has an algebraic solution in* $\mathbb{F}_p[\![x]\!]$.

($2_p$) *We have* $\deg a(x) < \deg b(x)$*, all poles of* $u(x)$ *are simple, and* $R(w)$ *splits completely in* $\mathbb{F}_p[w]$.

($3_p$) *We have* $u(x)^p + u^{(p-1)}(x) = 0$.

By Kronecker's Theorem: ($2_p$) for almost all prime numbers $p$ implies (2).

# Proof of Honda's Theorem

$$y'(x) = u(x)y(x) \quad \text{(Eq)} \quad \text{with } u(x) = \frac{a(x)}{b(x)}, \text{ and } R(w) \coloneqq \operatorname{Res}(b(x), a(x) - w \cdot b'(x)).$$

**Proposition (Folklore; Honda, 1981)**

*The following are equivalent:*

(1) (Eq) *has an algebraic solution.*

(2) *We have* $\deg a(x) < \deg b(x)$*, all poles of* $u(x)$ *are simple, and* $R(w)$ *splits completely in* $\mathbb{Q}[w]$.

**Proposition (Honda, 1981)**

*Let* $p$ *be a prime number. TFAE:*

($1_p$) $(\text{Eq})_p$ *has an algebraic solution in* $\mathbb{F}_p[\![x]\!]$.

($2_p$) *We have* $\deg a(x) < \deg b(x)$*, all poles of* $u(x)$ *are simple, and* $R(w)$ *splits completely in* $\mathbb{F}_p[w]$.

($3_p$) *We have* $u(x)^p + u^{(p-1)}(x) = 0$.

By Kronecker's Theorem: ($2_p$) for almost all prime numbers $p$ implies (2).

**Main question today:** Can we deduce (2) from ($2_p$) for a **finite** number of primes?

# An Effective Version of Kronecker's Theorem

**Theorem (Chudnovsky[2], 1985 )**

*Let $R(w) \in \mathbb{Z}[w]$ have leading coefficient $\Delta \in \mathbb{Z}_{>0}$.*

*Then* **there exists** $\sigma \in \mathbb{N}$ **such that** *the polynomial $R(w)$ splits completely in $\mathbb{Q}[w]$ if and only if $R(w)$ splits completely in $\mathbb{F}_p[w]$ for all primes $p$*

- *not dividing $\Delta$,*
- *bounded from above by $\sigma$.*

# An Effective Version of Kronecker's Theorem

**Theorem (Chudnovsky[2], 1985; F.-Pannier, 2025+)**

*Let $R(w) \in \mathbb{Z}[w]$ have leading coefficient $\Delta \in \mathbb{Z}_{>0}$, and let $t(\Delta) \coloneqq \prod_{p|\Delta} p^{1/(p-1)}$.*
*Let $B \in \mathbb{R}$ be an upper bound on the modulus of all complex roots of $R$.*
*Let $M \coloneqq \lceil 2.826 \cdot \Delta^3 \cdot t(\Delta)^3 \rceil$ and $N \coloneqq \lceil 6.076 \cdot BM \rceil$.*

*Then, setting $\sigma \coloneqq (2M+1)N + 2M$, the polynomial $R(w)$ splits completely in $\mathbb{Q}[w]$ if and only if $R(w)$ splits completely in $\mathbb{F}_p[w]$ for all primes $p$*

- *not dividing $\Delta$,*
- *bounded from above by $\sigma$.*

# An Effective Version of Kronecker's Theorem

**Theorem (Chudnovsky[2], 1985; F.-Pannier, 2025+)**

*Let $R(w) \in \mathbb{Z}[w]$ have leading coefficient $\Delta \in \mathbb{Z}_{>0}$, and let $t(\Delta) \coloneqq \prod_{p|\Delta} p^{1/(p-1)}$.*
*Let $B \in \mathbb{R}$ be an upper bound on the modulus of all complex roots of $R$.*
*Let $M \coloneqq \lceil 2.826 \cdot \Delta^3 \cdot t(\Delta)^3 \rceil$ and $N \coloneqq \lceil 6.076 \cdot BM \rceil$.*

*Then, setting $\sigma \coloneqq (2M+1)N + 2M$, the polynomial $R(w)$ splits completely in $\mathbb{Q}[w]$ if and only if $R(w)$ splits completely in $\mathbb{F}_p[w]$ for all primes $p$*

- *not dividing $\Delta$,*
- *bounded from above by $\sigma$.*

$$\frac{5\pi + \sqrt{25\pi^2 + 768\log(2)^2 - 384\log(2)\log(3)}}{8\log(2)} \approx 6.076$$

$$\sqrt[113]{955888052326228459135110382562803537966265345776 00} \approx 2.826$$

# An Effective Version of Kronecker's Theorem

## Theorem (Chudnovsky[2], 1985; F.-Pannier, 2025+)

*Let $R(w) \in \mathbb{Z}[w]$ have leading coefficient $\Delta \in \mathbb{Z}_{>0}$, and let $t(\Delta) := \prod_{p|\Delta} p^{1/(p-1)}$.*
*Let $B \in \mathbb{R}$ be an upper bound on the modulus of all complex roots of $R$.*
*Let $M := \lceil 2.826 \cdot \Delta^3 \cdot t(\Delta)^3 \rceil$ and $N := \lceil 6.076 \cdot BM \rceil$.*

*Then, setting $\sigma := (2M+1)N + 2M$, the polynomial $R(w)$ splits completely in $\mathbb{Q}[w]$ if and only if $R(w)$ splits completely in $\mathbb{F}_p[w]$ for all primes $p$*

- *not dividing $\Delta$,*
- *bounded from above by $\sigma$.*

## Corollary.

*If there is a* **single** *prime $p \leq \sigma$, not dividing $\Delta$, such that $R(w)$ does not split completely in $\mathbb{F}_p[w]$, then $R(w)$ does not split completely in $\mathbb{Q}[w]$.*

# Ideas of the Chudnovskys' Proof of Kronecker's Theorem

The function $x^\alpha = (1-z)^\alpha$ is algebraic if and only if $\alpha \in \mathbb{Q}$.

Given a root $\alpha \notin \mathbb{Q}$ of some polynomial $R(w) \in \mathbb{Q}[w]$, and two integers $M$ and $N$, **explicit Hermite-Padé approximants** $P_i(z) \in \mathbb{Q}(\alpha)[z]$ of degree at most $N$ are known such that

$$P_0(z) + P_1(z)(1-z)^\alpha + \cdots + P_{2M}(z)(1-z)^{2M\alpha} = g_\sigma z^\sigma + O(z^{\sigma+1}),$$

with $\sigma = (2M+1)N + 2M$, and $g_\sigma = \frac{N!^{2M+1}}{\sigma!} \in \mathbb{Q}^*$ [Hermite 1874; Jager, 1964].

# Ideas of the Chudnovskys' Proof of Kronecker's Theorem

The function $x^\alpha = (1-z)^\alpha$ is algebraic if and only if $\alpha \in \mathbb{Q}$.

Given a root $\alpha \notin \mathbb{Q}$ of some polynomial $R(w) \in \mathbb{Q}[w]$, and two integers $M$ and $N$, **explicit Hermite-Padé approximants** $P_i(z) \in \mathbb{Q}(\alpha)[z]$ of degree at most $N$ are known such that

$$P_0(z) + P_1(z)(1-z)^\alpha + \cdots + P_{2M}(z)(1-z)^{2M\alpha} = g_\sigma z^\sigma + O(z^{\sigma+1}),$$

with $\sigma = (2M+1)N + 2M$, and $g_\sigma = \frac{N!^{2M+1}}{\sigma!} \in \mathbb{Q}^*$ [Hermite 1874; Jager, 1964].

Let $L$ be the splitting field of $R(w)$. Construct $\Omega = \Omega_{M,N} \neq 0$ such that

$$|\mathrm{Norm}_{L/\mathbb{Q}}(\mathrm{num}(\Omega g_\sigma))| < X(M)^N \cdot Y(M) \text{ with } X(M) \to 0 \text{ as } M \to \infty.$$

# Ideas of the Chudnovskys' Proof of Kronecker's Theorem

The function $x^\alpha = (1-z)^\alpha$ is algebraic if and only if $\alpha \in \mathbb{Q}$.
Given a root $\alpha \notin \mathbb{Q}$ of some polynomial $R(w) \in \mathbb{Q}[w]$, and two integers $M$ and $N$, explicit Hermite-Padé approximants $P_i(z) \in \mathbb{Q}(\alpha)[z]$ of degree at most $N$ are known such that

$$P_0(z) + P_1(z)(1-z)^\alpha + \cdots + P_{2M}(z)(1-z)^{2M\alpha} = g_\sigma z^\sigma + O(z^{\sigma+1}),$$

with $\sigma = (2M+1)N + 2M$, and $g_\sigma = \frac{N!^{2M+1}}{\sigma!} \in \mathbb{Q}^*$ [Hermite 1874; Jager, 1964].

Let $L$ be the splitting field of $R(w)$. Construct $\Omega = \Omega_{M,N} \neq 0$ such that

$$|\mathrm{Norm}_{L/\mathbb{Q}}(\mathrm{num}(\Omega g_\sigma))| < X(M)^N \cdot Y(M) \text{ with } X(M) \to 0 \text{ as } M \to \infty.$$

But $\mathrm{num}(\Omega g_\sigma) \in \mathcal{O}_L^*$ has norm $\geq 1$, a **contradiction** for large $M$ and $N$. [Chudnovsky$^2$, 1985]

# Ideas of the Chudnovskys' Proof of Kronecker's Theorem

The function $x^\alpha = (1-z)^\alpha$ is algebraic if and only if $\alpha \in \mathbb{Q}$.
Given a root $\alpha \notin \mathbb{Q}$ of some polynomial $R(w) \in \mathbb{Q}[w]$, and two integers $M$ and $N$, explicit Hermite-Padé approximants $P_i(z) \in \mathbb{Q}(\alpha)[z]$ of degree at most $N$ are known such that

$$P_0(z) + P_1(z)(1-z)^\alpha + \cdots + P_{2M}(z)(1-z)^{2M\alpha} = g_\sigma z^\sigma + O(z^{\sigma+1}),$$

with $\sigma = (2M+1)N + 2M$, and $g_\sigma = \frac{N!^{2M+1}}{\sigma!} \in \mathbb{Q}^*$ [Hermite 1874; Jager, 1964].

Let $L$ be the splitting field of $R(w)$. Construct $\Omega = \Omega_{M,N} \neq 0$ such that

$$|\mathrm{Norm}_{L/\mathbb{Q}}(\mathrm{num}(\Omega g_\sigma))| < X(M)^N \cdot Y(M) \text{ with } X(M) \to 0 \text{ as } M \to \infty.$$

But $\mathrm{num}(\Omega g_\sigma) \in \mathcal{O}_L^*$ has norm $\geq 1$, a contradiction for large $M$ and $N$. [Chudnovsky[2], 1985]

**Our contribution [F.-Pannier, 2025+]**

Exhibiting explicit values of $M$ and $N$ such that the contradiction occurs.

# Effective Version of Honda's Theorem

**Corollary (Chudnovsky[2], 1985; F.-Pannier, 2025+)**

*Let* $a(x), b(x) \in \mathbb{Z}[x]$ *and* $R(w) := \mathrm{Res}_x(b(x), a(x) - w \cdot b'(x)) \in \mathbb{Q}[w]$, *with leading coefficient* $\Delta := |\mathrm{Res}_x(b(x), -b'(x))|$, $t(\Delta) := \prod_{p|\Delta} p^{1/(p-1)}$. *Let* $B \in \mathbb{R}$ *be an upper bound on the modulus of all complex roots of* $R$. *Let* $M := \lceil 2.826 \cdot \Delta^3 \cdot t(\Delta)^3 \rceil$ *and* $N := \lceil 6.076 \cdot BM \rceil$.

# Effective Version of Honda's Theorem

**Corollary (Chudnovsky[2], 1985; F.-Pannier, 2025+)**

*Let* $a(x), b(x) \in \mathbb{Z}[x]$ *and* $R(w) := \mathrm{Res}_x(b(x), a(x) - w \cdot b'(x)) \in \mathbb{Q}[w]$, *with leading coefficient* $\Delta := |\mathrm{Res}_x(b(x), -b'(x))|$, $t(\Delta) := \prod_{p|\Delta} p^{1/(p-1)}$. *Let* $B \in \mathbb{R}$ *be an upper bound on the modulus of all complex roots of* $R$. *Let* $M := \lceil 2.826 \cdot \Delta^3 \cdot t(\Delta)^3 \rceil$ *and* $N := \lceil 6.076 \cdot BM \rceil$.

*All solutions of* $y'(x) = \frac{a(x)}{b(x)} y(x)$ *are* **algebraic** *if and only if the* $p$-**curvatures** *of the equation vanish for all primes* $p$:

- *not dividing* $\Delta$
- *bounded from above by* $\sigma := (2M+1)N + 2M$.

# Effective Version of Honda's Theorem

## Corollary (Chudnovsky[2], 1985; F.-Pannier, 2025+)

*Let* $a(x), b(x) \in \mathbb{Z}[x]$ *and* $R(w) \coloneqq \mathrm{Res}_x(b(x), a(x) - w \cdot b'(x)) \in \mathbb{Q}[w]$, *with leading coefficient* $\Delta \coloneqq |\mathrm{Res}_x(b(x), -b'(x))|$, $t(\Delta) \coloneqq \prod_{p|\Delta} p^{1/(p-1)}$. *Let* $B \in \mathbb{R}$ *be an upper bound on the modulus of all complex roots of* $R$. *Let* $M \coloneqq \lceil 2.826 \cdot \Delta^3 \cdot t(\Delta)^3 \rceil$ *and* $N \coloneqq \lceil 6.076 \cdot BM \rceil$.

*All solutions of* $y'(x) = \frac{a(x)}{b(x)} y(x)$ *are* **algebraic** *if and only if the* $p$**-curvatures** *of the equation vanish for all primes* $p$*:*

- *not dividing* $\Delta$
- *bounded from above by* $\sigma \coloneqq (2M+1)N + 2M$.

## Proving Transcendence is Easy

A single prime suffices to conclude transcendence of the solutions.

# Algorithm and Complexity

**Input** $a, b \in \mathbb{Z}[x]$ of degree at most $d$, with coefficients bounded by $H$.

**Output** The nature (**algebraic** or **transcendental**) of $\exp(\int \frac{a}{b})$.

# Algorithm and Complexity

**Input** $a, b \in \mathbb{Z}[x]$ of degree at most $d$, with coefficients bounded by $H$.

**Output** The nature (**algebraic** or **transcendental**) of $\exp(\int \frac{a}{b})$.

1. **If** $b$ **not** squarefree or $\deg(a) \geq \deg(b)$ **then** return **transcendental**;
2. $R \coloneqq \mathrm{Res}_x(b, a - w \cdot b') \in \mathbb{Q}[w]$, $\Delta, t, B$;
3. $M \coloneqq \lceil 2.826 \cdot \Delta^3 \cdot t(\Delta)^3 \rceil$, $N \coloneqq 6.076 \cdot BM$, $\sigma \coloneqq (2M+1)N + 2M$, $p \coloneqq 2$;
4. **while** $p \leq \sigma$:
   i. **if** $p \nmid \Delta$, **then** compute the $p$-curvature;
   ii. **if** $p$-curvature $\neq 0$, **then** return **transcendental**, **else** $p \coloneqq \mathrm{nextprime}(p)$;
5. return **algebraic**.

# Algorithm and Complexity

**Input** $a, b \in \mathbb{Z}[x]$ of degree at most $d$, with coefficients bounded by $H$.

**Output** The nature (**algebraic** or **transcendental**) of $\exp(\int \frac{a}{b})$. $\tilde{O}(3^{-3d} d^{12d-1} H^{12d-6})$

1. **If** $b$ **not** squarefree or $\deg(a) \geq \deg(b)$ **then** return **transcendental**;
2. $R := \mathrm{Res}_x(b, a - w \cdot b') \in \mathbb{Q}[w]$, $\Delta, t, B$; $\tilde{O}(d^2 \log(H))$ bit operations
3. $M := \lceil 2.826 \cdot \Delta^3 \cdot t(\Delta)^3 \rceil$, $N := 6.076 \cdot BM$, $\sigma := (2M+1)N + 2M$, $p := 2$;
4. **while** $p \leq \sigma$: $\tilde{O}(d^2 \log H) \cdot \tilde{O}(B\Delta^6)$ bit operations [Bostan-Schost, 2009]
   i. **if** $p \not| \Delta$, **then** compute the $p$-curvature;
   ii. **if** $p$-curvature $\neq 0$, **then** return **transcendental**, **else** $p := \mathrm{nextprime}(p)$;
5. return **algebraic**.

$$t(\Delta) = O(\log \Delta), \quad \sigma = \tilde{O}(B\Delta^6), \quad B, \Delta = O(3^{-d/2} d^{2d-1/2} H^{2d-1})$$

# Algorithm and Complexity

**Input** $a, b \in \mathbb{Z}[x]$ of degree at most $d$, with coefficients bounded by $H$.

**Output** The nature (**algebraic** or **transcendental**) of $\exp(\int \frac{a}{b})$. $\tilde{O}(3^{-3d} d^{12d-1} H^{12d-6})$

1. **If** $b$ **not** squarefree or $\deg(a) \geq \deg(b)$ **then** return **transcendental**;
2. $R := \mathrm{Res}_x(b, a - w \cdot b') \in \mathbb{Q}[w]$, $\Delta, t, B$; $\tilde{O}(d^2 \log(H))$ bit operations
3. $M := \lceil 2.826 \cdot \Delta^3 \cdot t(\Delta)^3 \rceil$, $N := 6.076 \cdot BM$, $\sigma := (2M+1)N + 2M$, $p := 2$;
4. **while** $p \leq \sigma$: $\tilde{O}(d^2 \log H) \cdot \tilde{O}(B\Delta^6)$ bit operations [Bostan-Schost, 2009]
   i. **if** $p \not| \Delta$, **then** compute the $p$-curvature;
   ii. **if** $p$-curvature $\neq 0$, **then** return **transcendental**, **else** $p := \mathrm{nextprime}(p)$;
5. return **algebraic**.

$$t(\Delta) = O(\log \Delta), \quad \sigma = \tilde{O}(B\Delta^6), \quad B, \Delta = O(3^{-d/2} d^{2d-1/2} H^{2d-1})$$

"Generically", the algorithm takes $\tilde{O}(d^2 \log(H))$ bit operations to return **transcendental**.

# Preliminary Implementation in SageMath

| $a(x)/b(x)$ | Output | $p$ | $\sigma$ | Time |
|---|---|---|---|---|
| $\frac{1}{x^2+1}$ | **transcendental** | 3 | 25455734 | 17.1 ms |
| $\frac{3x-4}{x^2-3x+2}$ | **algebraic** | - | 265 | 120 ms |
| $\frac{1}{x^2-3818929}$ | **transcendental** | 57 | $7.922 \cdot 10^{46}$ | 88.7 ms |
| $\frac{2x+1}{x^2+x+1}$ | **algebraic** | - | 1926284 | 8 min 9 s |

```
[61]: a = 2*x+1
      b = x^2+x+1
      %time FullHonda1(a,b)

      Delta=3, t=1.73205080756888, B=1, M=397, N=2422
      sigma = 1926284
      CPU times: user 8min 9s, sys: 93.6 ms, total: 8min 9s
      Wall time: 8min 8s
[61]: 'algebraic'
```

# Preliminary Implementation in SageMath

| $a(x)/b(x)$ | Output | $p$ | $\sigma$ | Time |
|---|---|---|---|---|
| $\frac{1}{x^2+1}$ | **transcendental** | 3 | 25455734 | 17.1 ms |
| $\frac{3x-4}{x^2-3x+2}$ | **algebraic** | - | 265 | 120 ms |
| $\frac{1}{x^2-3818929}$ | **transcendental** | 47 | $7.922 \cdot 10^{46}$ | 88.7 ms |
| $\frac{2x+1}{x^2+x+1}$ | **algebraic** | - | 1926284 | 8 min 9 s |

```
[61]: a = 2*x+1
      b = x^2+x+1
      %time FullHonda1(a,b)

      Delta=3, t=1.73205080756888, B=1, M=397, N=2422
      sigma = 1926284
      CPU times: user 8min 9s, sys: 93.6 ms, total: 8min 9s
      Wall time: 8min 8s
[61]: 'algebraic'
```

# Indicial Polynomials – Abusing gfun's `istranscendental`

Working directly in the context of differential equations: $y(x)' = u(x)y(x)$:

The residues of $u(x)$ are the **local exponents** of the equation at its **singularities**. One can compute a degree one polynomial, the **indicial polynomial** in an algebraic extension of $\mathbb{Q}(x)$, at each of these singularities, whose sole zero is the local exponent.

# Indicial Polynomials – Abusing gfun's `istranscendental`

Working directly in the context of differential equations: $y(x)' = u(x)y(x)$:

The residues of $u(x)$ are the **local exponents** of the equation at its **singularities**. One can compute a degree one polynomial, the **indicial polynomial** in an algebraic extension of $\mathbb{Q}(x)$, at each of these singularities, whose sole zero is the local exponent.

**Proposition**

The solution of $y'(x) = u(x)y(x)$ for $u(x) \in \mathbb{Q}(x)$ is algebraic if and only if the equation is **Fuchsian** and all local exponents are rational.

# Indicial Polynomials – Abusing gfun's `istranscendental`

Working directly in the context of differential equations: $y(x)' = u(x)y(x)$:

The residues of $u(x)$ are the **local exponents** of the equation at its **singularities**. One can compute a degree one polynomial, the **indicial polynomial** in an algebraic extension of $\mathbb{Q}(x)$, at each of these singularities, whose sole zero is the local exponent.

**Proposition**

The solution of $y'(x) = u(x)y(x)$ for $u(x) \in \mathbb{Q}(x)$ is algebraic if and only if the equation is **Fuchsian** and all local exponents are rational.

**Upshot:** "Easy" calculations in an algebraic extension of $\mathbb{Q}$ give an algorithm to decide algebraicity of solutions.

# Indicial Polynomials – Abusing gfun's `istranscendental`

Working directly in the context of differential equations: $y(x)' = u(x)y(x)$:

The residues of $u(x)$ are the **local exponents** of the equation at its **singularities**. One can compute a degree one polynomial, the **indicial polynomial** in an algebraic extension of $\mathbb{Q}(x)$, at each of these singularities, whose sole zero is the local exponent.

**Proposition**

The solution of $y'(x) = u(x)y(x)$ for $u(x) \in \mathbb{Q}(x)$ is algebraic if and only if the equation is **Fuchsian** and all local exponents are rational.

**Upshot:** "Easy" calculations in an algebraic extension of $\mathbb{Q}$ give an algorithm to decide algebraicity of solutions.

`gfun` package for Maple has command `istranscendental` deciding transcendence of solutions of arbitrary order equations based on [Bostan, Salvy, Singer 2025+]. Can be "abused" for order one equations to check the conditions from the Proposition above.

# The Least Prime That Does Not Split in a Number Field

Given a Galois field extension $K/\mathbb{Q}$ of degree $d \neq 1$ and discriminant $D$, estimates on the size of the smallest prime that does not split completely in $K$ are known.

# The Least Prime That Does Not Split in a Number Field

Given a Galois field extension $K/\mathbb{Q}$ of degree $d \neq 1$ and discriminant $D$, estimates on the size of the smallest prime that does not split completely in $K$ are known.

## Theorem (Valer, Voloch, 2000)

*If* $\exp(\max\{105, 25(\log(d))^2\}) \leq 8D^{\frac{1}{2(d-1)}}$ *then there exists a prime* $p$*, such that* $p$ *does not split completely in* $K$ *and* $p \leq 26d^2 D^{\frac{1}{2(d-1)}}$.

# The Least Prime That Does Not Split in a Number Field

Given a Galois field extension $K/\mathbb{Q}$ of degree $d \neq 1$ and discriminant $D$, estimates on the size of the smallest prime that does not split completely in $K$ are known.

**Theorem (Valer, Voloch, 2000)**

*If* $\exp(\max\{105, 25(\log(d))^2\}) \leq 8D^{\frac{1}{2(d-1)}}$ *then there exists a prime* $p$*, such that* $p$ *does not split completely in* $K$ *and* $p \leq 26d^2D^{\frac{1}{2(d-1)}}$*.*

Apply this to the splitting field of the Rothstein-Trager resultant:

A prime $p$ splitting completely in the splitting field of a polynomial $R(w)$ is equivalent to $R(w) \bmod p$ splitting into linear factors in $\mathbb{F}_p[w]$.

# The Least Prime That Does Not Split in a Number Field

Given a Galois field extension $K/\mathbb{Q}$ of degree $d \neq 1$ and discriminant $D$, estimates on the size of the smallest prime that does not split completely in $K$ are known.

**Theorem (Valer, Voloch, 2000)**

*If* $\exp(\max\{105, 25(\log(d))^2\}) \leq 8D^{\frac{1}{2(d-1)}}$ *then there exists a prime* $p$*, such that* $p$ *does not split completely in* $K$ *and* $p \leq 26d^2 D^{\frac{1}{2(d-1)}}$*.*

Apply this to the splitting field of the Rothstein-Trager resultant:

A prime $p$ splitting completely in the splitting field of a polynomial $R(w)$ is equivalent to $R(w) \bmod p$ splitting into linear factors in $\mathbb{F}_p[w]$.

**Obstacles:** impractical bounds, the discriminant of a polynomial does not directly relate to the discriminant of its splitting field.

# Finding Rational Roots

**Theorem (Bostan, Chyzak, Giusti, Lebreton, Lecerf, Salvy, Schost, 2017)**

*Finding all rational roots of a monic univariate polynomial $R(w) \in \mathbb{Z}[w]$ of degree $d$, whose coefficients are bounded by $H \in \mathbb{N}$ can be done in*

$$\tilde{O}(d^2 \log(H))$$

*bit operations where the notation $\tilde{O}$ hides logarithmic factors $\log(d)$ and $\log(\log H)$.*

**Corollary**

*Let $u(x) \in \mathbb{Q}(x)$ be of degree $d$, with coefficients bounded by $H$. One can decide in $\tilde{O}(d^3 \log(H))$ bit operations if its residues are rational by finding all rational roots of the Rothstein-Trager resultant, or, equivalently, if the associated equation $y'(x) = u(x)y(x)$ has algebraic solutions.*

**Recall our complexity:** $\tilde{O}(3^{-3d} d^{12d-1} H^{12d-6})$ **:(**

# Small Examples – Timings

| $a(x)/b(x)$ | $\sigma$ | Output | $p$-curv | ist | fact | RR |
|---|---|---|---|---|---|---|
| $\frac{3x-4}{2x^2-6x+4}$ | $265$ | **algebraic** | $120$ ms | $45$ ms | $< 1$ ms | $25$ ms |
| $\frac{7x^2-3x-4}{2x^3+4x^2-6x+4}$ | $\approx 6 \cdot 10^{27}$ | **transcendental** | $5$ ms | $38$ ms | $< 1$ ms | $30$ ms |
| $\frac{2x+1}{x^2+x+1}$ | $1926284$ | **algebraic** | $8$ min $9$ s | $19$ ms | $< 1$ ms | $24$ ms |
| $\frac{1}{x^2-4}$ | $\approx 10^{11}$ | **algebraic** | DNF | $15$ ms | $< 1$ ms | $22$ ms |

# Large Examples – Timings

Random large inputs almost always yield output **transcendental**.

| Degree | Height | $p$-curv | ist | RT+RR (Maple) RT | RT+RR | fact (Sage) |
|---|---|---|---|---|---|---|
| 10 | $2^{10}$ | 1 ms | 12 ms | 3 ms | 3 ms | $< 1$ **ms** |
| 20 | $2^{10}$ | 2 **ms** | 24 ms | 9 ms | 10 ms | 4 ms |
| 20 | $2^{20}$ | 2 **ms** | 25 ms | 19 ms | 21 ms | 7 ms |
| 40 | $2^{10}$ | 4 **ms** | 71 ms | 46 ms | 49 ms | 79 ms |
| 40 | $2^{20}$ | 5 **ms** | 76 ms | 100 ms | 107 ms | 171 ms |
| 80 | $2^{10}$ | 0.1 **s** | 0.3 s | 0.3 s | 0.3 s | 2.4 s |
| 80 | $2^{20}$ | 0.1 **s** | 0.3 s | 0.6 s | 0.6 s | 5.0 s |
| 160 | $2^{10}$ | 0.4 **s** | 1.8 s | 2.4 s | 2.4 s | 83 s |
| 160 | $2^{20}$ | 0.4 **s** | 1.9 s | 3.9 s | 4.0 s | 182 s |

**Our algorithm quickly proves transcendence.**

# The End

**Future:** Make the Grothendieck conjecture effective for all the cases in which it is known.

Thank you for your attention!

# Bonus – Exceptional Primes

## Example

Consider

$$u(x) = \frac{a(x)}{b(x)} = \frac{x+2}{2x^2+x-1} = \frac{5}{6} \cdot \frac{1}{x-\frac{1}{2}} - \frac{1}{3} \cdot \frac{1}{x+1}.$$

# Bonus – Exceptional Primes

## Example

Consider

$$u(x) = \frac{a(x)}{b(x)} = \frac{x+2}{2x^2+x-1} = \frac{5}{6} \cdot \frac{1}{x-\frac{1}{2}} - \frac{1}{3} \cdot \frac{1}{x+1}.$$

The equation $y'(x) = u(x)y(x)$ has the algebraic solution

$$y(x) = \frac{(2x-1)^{5/6}}{(x+1)^{1/3}},$$

which can be reduced modulo all primes numbers except for $2$ and $3$.

# Bonus – Exceptional Primes

## Example

Consider

$$u(x) = \frac{a(x)}{b(x)} = \frac{x+2}{2x^2+x-1} = \frac{5}{6} \cdot \frac{1}{x-\frac{1}{2}} - \frac{1}{3} \cdot \frac{1}{x+1}.$$

The equation $y'(x) = u(x)y(x)$ has the algebraic solution

$$y(x) = \frac{(2x-1)^{5/6}}{(x+1)^{1/3}},$$

which can be reduced modulo all primes numbers except for $2$ and $3$.
We have $\Delta = \mathrm{Res}_x(b(x), -b'(x)) = -18$.

# Bonus – Exceptional Primes

## Example

Consider

$$u(x) = \frac{a(x)}{b(x)} = \frac{x+2}{2x^2+x-1} = \frac{5}{6} \cdot \frac{1}{x-\frac{1}{2}} - \frac{1}{3} \cdot \frac{1}{x+1}.$$

The equation $y'(x) = u(x)y(x)$ has the algebraic solution

$$y(x) = \frac{(2x-1)^{5/6}}{(x+1)^{1/3}},$$

which can be reduced modulo all primes numbers except for $2$ and $3$.
We have $\Delta = \mathrm{Res}_x(b(x), -b'(x)) = -18$. For $p = 2$ the denominator of $u(x)$ reduces to a degree one polynomial.

# Bonus – Exceptional Primes

## Example

Consider

$$u(x) = \frac{a(x)}{b(x)} = \frac{x+2}{2x^2+x-1} = \frac{5}{6} \cdot \frac{1}{x-\frac{1}{2}} - \frac{1}{3} \cdot \frac{1}{x+1}.$$

The equation $y'(x) = u(x)y(x)$ has the algebraic solution

$$y(x) = \frac{(2x-1)^{5/6}}{(x+1)^{1/3}},$$

which can be reduced modulo all primes numbers except for $2$ and $3$.
We have $\Delta = \mathrm{Res}_x(b(x), -b'(x)) = -18$. For $p = 2$ the denominator of $u(x)$ reduces to a degree one polynomial. For $p = 3$ the two poles $x = \frac{1}{2}$ and $x = -1$ collapse to a single pole of order $2$.